Incident Response Plan Guidance Document

7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73

September 4, 2014

Centers for Disease Control and Prevention
(CDC) Division of Select Agents

Preface

Revisions: This is a living document subject to ongoing improvement. Feedback or suggestions for improvement from registered Select Agent entities or the public are welcomed. Please submit comments directly to the Federal Select Agent Program at:

CDC: LRSAT@cdc.gov
APHIS: ASAP@aphis.usda.gov

Revision History:

October 12, 2012: Initial posting
June 19, 2013 (Revision 1): The revisions are primarily changes to correct editorial errors from previous version.
February 10, 2014: Added "Low probability/High consequence Events" to Appendix IV.
September 4, 2014: Added information about continuing laboratory operations after incident.

Introduction

Under the provisions of select agent regulations (7 CFR §331.14, 9 CFR §121.14 and 42 CFR §73.14), an entity registered with the Federal Select Agent Program is required to have plans in place in the event of a natural and/or man-made disaster. With these provisions the Federal Select Agent Program can, with reasonable comfort, be assured that the select agents and toxins, which are in the possession of these entities are routinely secured and safeguarded under watchful eyes.

However, in the evaluation of the regulated entities, the likelihood of a direct man-made threat (i.e., direct attack with the intent to steal select agents and toxins that have a high probably for use as a weapon of mass destruction) is low. Unfortunately, the same cannot be said for natural disasters. A natural disaster is more likely to threaten a registered entity with the potential for releasing a select agent or toxin into the environment making the risk of human, animal or plant health exposures possible.

This guide is to assist the regulated community in developing a site-specific incident response plan to ensure the security and safeguarding of select agents and toxins from natural and man-made disasters.

Table of Contents

Section 1: Five Keys to successful incident response

1) It is focused on protecting human life before property
2) It is focused on the impact to the laboratory and not just the facility
3) It is the result of collaboration between entity leadership and responders
4) The responders participate in entity training
5) It addresses the primary effect of the hazard, the secondary effects, and the effect it has on the people who work at the facility

Section 2: What is an 'incident response' plan?

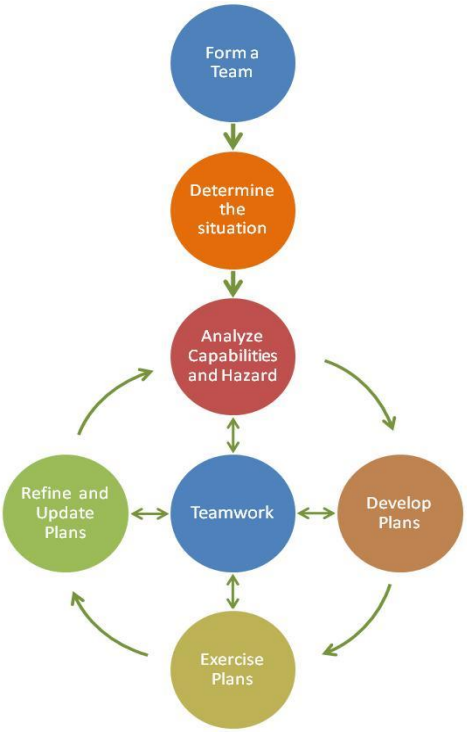
An incident response plan is nothing more than a set of standard operating procedures (SOPs). It is a key part of risk management, a way of planning for the hazards that cannot effectively be mitigated. ***An incident is an occurrence, natural or manmade, that requires a response to prevent the theft, loss or release of the select agent or toxin or to protect human life, and animal and plant health.*** The incident response plan should focus on areas inside the laboratory or registered space.

The Federal Select Agent Program requires an incident response plan for certain incidents. As with the written security plan, the incident response plan must be site-specific which means that each section of the written plan must be a reflection of risk identified in the site-specific risk assessment and the entity's actual policies and procedures relating to incident response. In developing the written incident response plan, the entity needs to factor in the agent specific consequence assessment as documented in the entity's written security plan.

The entity's incident response plan must contain all of the requirements outlined in the select agent regulations. This includes theft, loss, or release of a select agent or toxin, inventory discrepancies, security breaches (including information systems), natural disasters, workplace violence, bomb threats, suspicious packages, and emergencies such as fire, gas leak, explosion, power outage, among others. Appendix I contains more detailed instructions on how to meet these requirements. Appendix VI contains a checklist to assist in compliance.

There are other statutes (federal, state and local government) that address emergency and incident response. The select agent incident response plan is not intended to preempt or supersede other response agreements or written plans provided that other plans and agreements address the requirements of section 14 of the select agent regulations. If an entity chooses to use other plans as a means of meeting these requirements, section 18 of the select

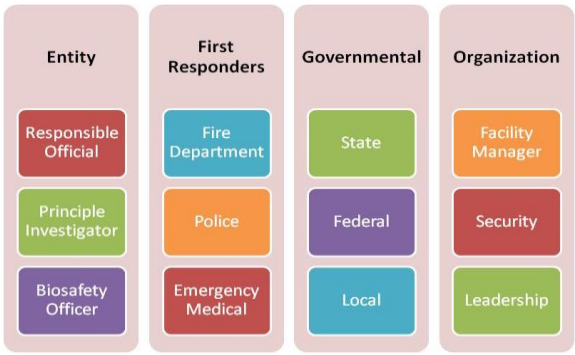
agent regulations requires that this information be made available to Federal Select Agent Program inspectors when on-site inspections are conducted.



Section 3: The Incident Response Planning Cycle

Incident response planning may be viewed as a six step cycle. It begins with the formation of a team of subject matter experts (SMEs) and stakeholders. First, the team analyzes the team's capabilities and all unmitigated hazards (human and natural). Next, the team develops an SOP or series of SOPs and plans for the incidents. Finally, the plan is exercised and modified at least annually.

Step 1: Form a team

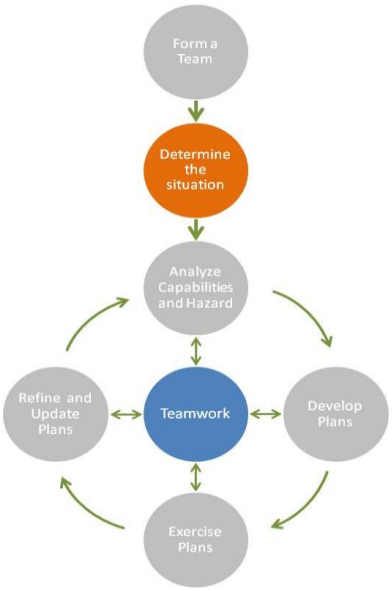


The first step is to form a team of both entity SMEs, supporting SMEs and stakeholders. The team should include entity professionals who are experts on the consequences of the agents and how the entity operates (its SOPs). The team should also include first responders knowledgeable of what capabilities they bring to the response effort. It may also include facilities managers and security personnel familiar with how the organization as a whole responds. Finally, the entity may want to bring in state and federal partners as well.

Once the team is formed, it should remain engaged throughout the process. Each team member brings both skills and a unique perspective to the situation. At each step, the entity is strongly encouraged to consult team members.

Step 2: Determine the current situation

The process begins with the SMEs and stakeholders determining where they stand. The entity identifies risks (probable hazards, high consequence events) that cannot be mitigated before a response is required. This should include those required by regulation (see Appendices I and II), regional natural disasters (see Appendix III) along with other hazards identified in the site-specific risk assessment. The entity also identifies what protective measures/equipment they have in place and where they are located. Finally, the entity should be prepared to discuss its own SOPs which affect incidents. This includes 'man-down' drills, evacuation procedures and others.



The first responders also provide critical information. They should be able to talk about what capability they bring (HAZMAT, Police). Also, they should be able to talk about their own SOPs and policies (e.g., HAZMAT decontamination requirements). They should know response times to the entity by hazard type for multiple situations. Finally, they should also discuss contact and communication procedures beyond calling 911 (see Appendix III).

Facility management along with organizational safety and security personnel provide the final piece(s) of information. They should know the physical capabilities of the building(s) and what emergency equipment they have on hand. This includes existing policies and organizational wide procedures for managing incidents. This may include a 'workplace violence' policy and memorandum of agreement with first responders. Finally, they may be the ones who must escort or otherwise grant access to first responders.

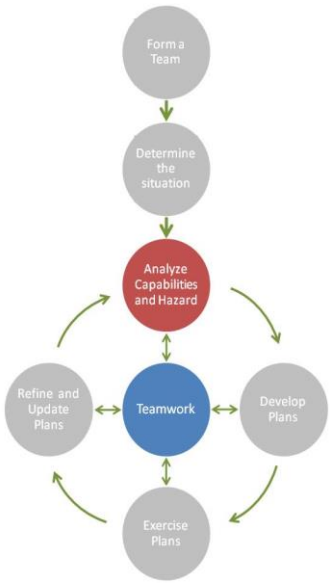
For natural hazards, there is information available from the federal government. Appendix III includes lists of sites the entity should check along with suggested procedural steps. This includes 'hazard zone' for tornadoes, hurricanes and earthquakes. Beyond that, the suggested websites can give information such as flood and tidal surge (storm surge) maps. Entities should be aware of what hazards may directly impact their registered areas (labs, storage areas) along with the impacts of the event on their people and surrounding infrastructure (roads, power, etc.). Entities should also be aware and prepared for externalities of natural hazards as displayed in Appendix IV.

The entity should begin the discussion by describing itself to the responders. A physical walk through of the laboratory is recommended but rarely possible. Hence, entities should describe the layout of the registered spaces and the physical makeup of the facility to include "Hot" or "No-Go" areas and warning signs.

Step 3: Analyze Capabilities against Hazards

The next step is to weigh capabilities against hazards. The Federal Select Agent Program requires the entity address certain hazards identified in Appendices I and II. They can form the core of an incident response plan. Beyond that, the entity should also identify any risks that cannot be mitigated from the site specific risk assessment.

A simple means of conducting this analysis is through scenarios. These are a series of incident driven actions and events and provide a factual and logical framework for developing an SOP. The scenarios can assist in guiding discussion and help sequence response actions.



Scenarios can be analyzed in a number of ways. They could be "action/response" based where each action leads to a reaction and so on until the tasks are complete. They can also be "functionally" based, where each organization talks through its internal SOPs and determines where they should overlap. They can be a "walk-through", where the team can actually see what's available, where equipment sits and where the clean/dirty areas are.

The analysis should also address second order effects to the entity. In simple terms, incidents lead to other incidents. An earthquake may cause a long term power outage or fire. A hurricane evacuation may prevent access to the facility. A fire suppression system may flood the effluent containment system. A break-in may damage biosafety cabinets. These factors should be discussed as the team moves through the scenario.

Scenarios should focus on key questions. Obviously, it should focus on "who must do what, when and where." But it should also define information requirements, what do the team members need to know and who conveys the message (i.e., are all personnel evacuated and accounted for? Is the lab "clean"? How (i.e., phone, text, face-to-face)?). Beyond that, the scenario should answer equipment questions (How many HAZMAT suits do we need?). It should also define who's "in charge" at each step and what decisions have to be made when (i.e., let the structure burn).

As part of this analysis, the entity should document both expectations and assumptions for all team members. These are important because if they are not met, the plan may not work. For example, if the entity assumes the access roads will be clear, that should be noted. If first responders expect another organization to support the incident, that should be noted as well.

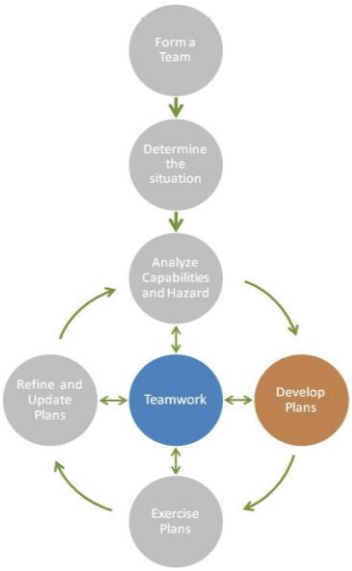
Also, the entity should identify constraints. These are things the response team(s) must do or cannot do. For example, if the entity has a person with special needs, they may not be able to evacuate on their own so they must get help. If the police do not have Personal Protective Equipment (PPE) or are not trained to use it, they must not enter the laboratory.

This analysis may lead to capability gaps. These are required capabilities the team members do not have. The scenario may identify a need for specialized HAZMAT gear the first responder's lack. If the entity finds they lack access to critical equipment, they are encouraged to reach out and add team members who have this equipment.

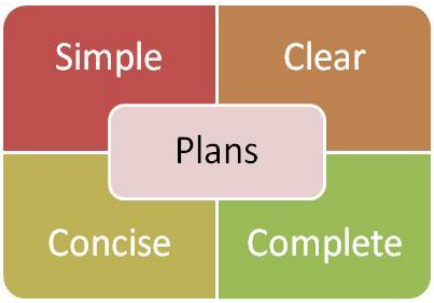
Finally, the entity should focus on the inside of the laboratory, not simply the structure. Building codes will generally ensure the facility can survive any probable disaster. However, they will not address loss of primary and secondary containment, animal husbandry issues, spilled vials of agent, loss of power to a freezer, etc.

Step 4: Develop a plan(s) by incident type.

The next step is to develop a plan or series of plans based on the scenarios. Plans do not have to be complex and more is not necessarily better. Plans should be simple only containing the required steps. They should be clear so that anyone can understand them. They should be concise and easy to read by laboratorians and responders alike. Finally, they should be complete covering all required hazards and meeting all regulatory requirements.



To meet this end state, entities are encouraged to develop playbooks. A playbook is a series of simple plans / SOPs that cover the multiple incidents identified in the analysis stage. The responses are 'layered' based on the incident. Similar to a "Playbook" they are common procedures or strategies which apply to multiple situations. Instead of focusing on nuances of each event, an entity can focus on common steps and then apply them to various incidents. This not only makes incident response easier for individuals to understand it also makes it much easier to train.



For example, an entity may have three incident response SOPs. The first is "without notice" where entity personnel evacuate immediately without doffing PPE and would include explosion, gas leak, workplace violence and possibly fire. The second could be "with minimal notice" where entity personnel can doff PPE and secure but not evacuate the select agents or toxins. This may include minor earthquake, tornado, civil disturbance or possibly fire. The third could be "with notice." In this case, the select agent can be safely secured or evacuated to an alternate location. An example would be a hurricane or flood.

Entities can also modify existing organizational plans to meet laboratory conditions. Many organizations have existing plans which can be quickly modified to suit laboratory requirements. Using this technique ensures agreement with other organizational policies. However, with this technique, the entity must modify its plan every time the organizational plan changes.

Entities can also create a different plan for each incident and regulatory requirement. An entity could then cover the nuances of each scenario and direct specific actions based upon them. This allows for a detailed understanding of many SOPs.

Finally, there are incidents which don't fit cleanly into a playbook. They may be laboratory-specific and not organization wide. These are usually for regulatory reason or because of organizational policy. For example, Section 14 requires the entity address theft/loss/release or inventory discrepancy. State and local governments may have additional requirements as well. The entity may have to create a separate document for these requirements.

Regardless of the method, each plan/play should contain common information (see Appendix II for detailed discussion):

1. What incidents the plan covers?
2. Concept (What are you trying to do? When are you done?)
3. Entity and organizational responsibilities/tasks (What will the entity do? Who does it/when? What is the entity responsible for?)
4. First responder actions/tasks (What will they/won't they do?)
5. Entity lines of authority (Who has the authority to call this kind of response? Who's next in charge?)
6. Decontamination procedures (Do you doff? If not, how do you separate contaminated personnel?)
7. Emergency equipment (Where is it? How does it apply? Who uses it?)
8. Procedures for emergency evacuation, including type of evacuation, exit route assignments, safe distances, and places of refuge (How do you get out? Where do you go once you leave the lab?)
9. Personnel accountability (Who accounts for personnel and who is notified once personnel are accounted for?)
10. Procedures to be followed by employees performing rescue or medical duties and the location (Where do you conduct immediate care? Where do you conduct follow up?)
11. Location where the first responders will pick up a patient and what amount of decontamination must be done (Doffing, showering out—consult the first responders on their requirements for transport)
12. Contacts and communication plan (Who calls 911? Who notifies the RO or management? Is anyone else notified?)
13. Site security and control (How do you manage access to the facility during and after the incident, where's the perimeter, etc.?)
14. Return procedures (Under what conditions and how do you return to the lab, check containment, etc.)
15. Select agent and toxin (and other high value items) accountability
16. Medical Surveillance (if required)

Incidents that are natural or man-made may arise at any time causing little to major damage to an area. Incident Response plans usually focus on how to protect from, prepare for, respond to, recover from and/or mitigate natural or man-made emergencies. To address the recovery phase, the Incident Response Plan should include procedures for emergencies that would prevent entities from returning to normal operating conditions (e.g., laboratory damaged by tornado and is not operational after an incident). Specifically, the response portion of the plan should address the following questions:

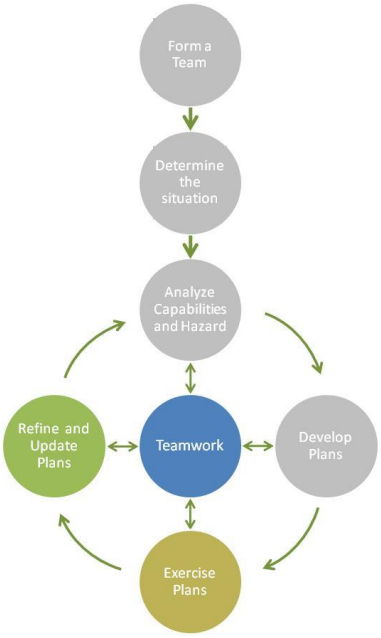
- What happens when laboratory cannot be return to business as usual after an incident?
- When will the laboratory be able to return to work?
- Will work with select agents and toxins continue in another registered space?
- Will select agents and toxins be stored in another registered space until the damaged area is operational?
- Will select agents and/or toxins be transferred to another registered entity until the damaged laboratory is operational?

Once the plan is drafted, it should be reviewed for completeness. The plan should cover all identified scenarios and meet all regulatory requirements (see Appendices V and VI for an example of cross walks). It should also have each team member's task(s) and purpose(s) for each step of the process. If the team made critical assumptions, they should be noted as well. Finally, it should be written in a way that anyone (not just the team members) can understand.

Once the plan is complete, the entity should get buy-in from the team members' leadership and other stakeholders. Leaders should acknowledge their responsibilities and confirm that they have the capability to carry them out. Stakeholders should concur with the concept of the plan and ensure it does not conflict with other policies.

Step 5: Exercise the plan

The Federal Select Agent Program requires the entity exercise their plan at least annually. This may be a table top, a walkthrough, a drill or a full scale exercise. Regardless, entities are strongly encouraged to have representatives from all of the planning team's organizations participate. This should include the first responders, key organizational members (facilities management, security, etc.) along with all entity personnel.



This is another reason to focus the plans. Simple SOPs based on common steps allow an entity to focus its valuable training time on the most important tasks. The team members (first responders) have less training overhead as well. Finally, it may be better to

be very good with a few key SOPs than marginal on many.

Step 6: Refine and Update Plans

Entities must refine and update their plan(s) at least annually, after each exercise or after a plan is executed. This is not a matter of resigning the document; the entity should revalidate or modify the plan. To do this, entities should re-establish the planning team of SMEs and stakeholders and go through the cycle again. Though they do not need to re-write the plan, they should address any changes that occurred during the year. They should address at minimum:

- ❑ Results of training (what went well, what can be improved, changes made)
- ❑ Any changes to threats or hazards
- ❑ Any changes to expectations or assumptions from the original plan
- ❑ Any new equipment, its capabilities and locations including first responders (new PPE, new HAZMAT vehicle)
- ❑ Any changes to the entity (additional registered space)
- ❑ Any changes in key personnel or organizations, including first responders
- ❑ Changes to the agents which affect response (adding a Tier 1 agent)
- ❑ Specific threats against the entity or its personnel
- ❑ Any changes in communications
- ❑ Critical changes to regulatory requirements, including those which affect first responders

References

1. CDC: http://www.cdc.gov/niosh/topics/emres/business.html
2. FEMA: http://www.fema.gov/
3. National Incident Management System, 2008
4. NOAA: http://www.noaa.gov/
5. USGS: http://www.usgs.gov/
6. SBA: http://www.sba.gov/category/navigation-structure/starting-managing-business/managing-business/running-business/emergency-preparedness-and-disaster-

Appendices

The information found in the appendices consists of information that an entity may consider in the development and implementation of Incident Response Plan. The user is not required to use, or limited to, the information provided in the appendices.

Appendix I. Regulatory Requirements

Section 14 (b) Requirements:

The incident response plan must fully describe the entity's response for the following procedures in the chart below.

Incident	Definition of Incident	Examples	Incident Notice
Theft, loss or release of a select agent or toxin	**Theft:** Unauthorized removal of select agent or toxin. **Loss:** A failure to account for select agent or toxin **Release:** A discharge of a select agent or toxin outside the primary containment barrier due to a failure in the containment system, an accidental spill, occupational exposure, or a theft. Any incident that results in the activation of a post exposure medical surveillance/prophylaxis protocol should be reported as a release.	Vial containing select agent missing or stolen; spills; needle stick;	No Notice
Inventory discrepancies	Inventory discrepancies occur when inventory (e.g., vials, containers) do not match the record data.	Mislabeled vials	No Notice
Security breaches/ Suspicious Activity	A security breach occurs when there is a disruption in the established security network or a failure to follow the entity's written security policies and procedures. Breaches involve all levels of security including physical security (hardened, fixed systems), operational security (personnel reliability) and information systems (electronic and hard copy material).	Computer hacking; unauthorized personnel in laboratory	No Notice
Severe weather and other natural disasters	Severe weather and natural disasters vary from one geographic location to another within the United States. Severe weather situations and natural disasters include tropical storms, hurricanes, tornadoes, windstorms, thunderstorms, lightning, hail, floods, earthquakes, fires and winter storms (not all inclusive). To assist in determining if the entity is in an affected area, refer to Tab IV "Evaluating Natural Hazard."	Tornado Warnings; Flood Warnings	Minimal Notice for tornado, severe weather or storm, hurricane, floods No Notice for earthquakes
Bomb Threats	Bomb threats have become common means to disrupt workplace activity. Most agencies at the academic, state, and federal levels have their own bomb threat policy.	Any object that appears suspicious or looks like it might be explosive.	Minimal Notice
Gas leak	A gas leak is a non-expected release of gas that can create a potentially dangerous situation - either because the released gas is poisonous or because it can ignite and create an explosion.	Smell of gas; sound of air being released from an open gas valve	Minimal Notice
Explosion	Explosion is the sudden loud release of energy and a rapidly expanding volume of gas that occurs when a bomb detonates or gas explodes	Bomb detonates or gas explodes	No Notice

Section 14 (c) Requirements:

Emergency Contact Information

When developing critical emergency contact information the entity needs to assess the roles and responsibilities of each identified person. The structure should be concise and easily understood in order to facilitate the activation of the incident response plan. All contact information should be site-specific and focused on support units that are available within the geographic region of the facility, especially if the entity is relying on local support of first responders. Entities that are associated with larger parent organizations (i.e., colleges, universities, federal or state campuses and research medical institutions) need to incorporate or integrate their site-specific incident response requirements with established entity-wide emergency response programs. This integration will assure that when emergency services are required, the first responders will be familiar with the requirements of the site-specific plan. Appendix 4 is a sample matrix for contact information required in Section 14 (c).

Personnel roles and lines of authority and communication

During an actual incident, arbitrarily assigning responsibilities would lead to inconsistencies and most likely result in a less than favorable outcome. For this reason roles and responsibilities need to be identified beforehand. In addition to roles and responsibilities, it is important that all participants understand the lines of authority and how information is communicated both up and down the chain of command.

Planning and coordination with local emergency responders

In addition to the information included in the select agent and toxin hazards section listed above, the importance of meeting with local emergency responders to discuss large scale disasters is important. An incident such as a hurricane or tornado could trigger a national emergency which could directly affect the select agent laboratory. It is important that discussions with local responders include these types of disasters and an agreement reached regarding the roles and responsibilities of each party.

Procedures to be followed by employees performing rescue and medical duties

Rescue and medical duties should be limited to only those individuals that are qualified to perform these duties (paramedic, EMT, registered nurse, physician assistant, medical doctor, osteopathic physician). When qualified individuals are not available, 911 should be called. Training staff to perform emergency first aid and CPR may be a consideration in laboratories that are located in remote areas that do not have 911 services or there is a delayed ambulance response time.

Emergency medical treatment and first aid

The incident response plan needs to establish provisions for emergency medical treatment and first aid for employees injured on the job. Since occupational injuries and illnesses are work related, worker's compensation rules may apply. It is important to check with the personnel department (human resources) to determine if employees have to report to a prearranged emergency treatment center or clinic. In any event, workers need to know where to go or be transported for emergency medical treatment or first aid. In laboratories that are regulated by state or federal OSHA (Occupational Safety and Health Administration), an injury log (e.g., OSHA 300) will be required to record all injuries that result in lost time or in medical treatment.

List of personal protective and emergency equipment, and their locations

The incident response plan needs to identify what personal protective equipment (PPE) and emergency equipment is needed and state where it is located. The laboratory should consider including a floor plan showing the PPE and emergency equipment locations. Examples of PPE include, but are not limited to: gloves, protective eyewear, face shields, respirators, foot protection, gowns, and scrubs. Examples of emergency equipment include, but are not limited to: fire extinguishers, emergency showers, fire blankets, eye wash stations, and portable lighting.

Site security and control

When an incident occurs, regardless of size, site security and control must be maintained. There may be a tendency to overlook site security due to the urgency to bring an incident under control. This is another instance where planning with the local responders is important. First responders need to know that access to restricted areas needs to be controlled during and after each incident. Some of the typical methods used to maintain site security control include a posted armed police officer or guard, yellow "caution" tape around the perimeter, "keep out" signs, emergency lighting, etc.

Procedures for emergency evacuation

Whether select agent related or not, the incident response plan should define the different types of evacuations that may be encountered such as fire, bomb, chemical spill, hostage, civil disturbance, explosion, etc. Floor plans that show the primary and secondary emergency exit routes should be posted on each floor and included in the incident response plan. Employees need to evacuate to areas that are safely out of harm's way to the designated assembly area for roll call verification. In determining safe distances for evacuation the worst case scenario should be considered. When a warning is received regarding an impending disaster, the incident response plan should designate areas for safe refuge until the warning expires or the threat no longer exists.

Decontamination procedures

Decontamination procedures need to be described in the incident response plan and should include a decontamination procedure for spills, injured select agent workers, emergency responders and laboratory rooms and areas that require mass decontamination.

Annual Training

Annual incident response training for personnel who have access to select agents or toxins must be provided and documented by the Responsible Official or designee. The documentation of incident response training must include: name of trained personnel, date, name of training, and how it verified that personnel understood training goals and objectives. For entities with Tier 1 agents insider threat awareness training must be conducted annually with all personnel who have access to select agents or toxins.

Tier 1 Requirements

Entities with Tier 1 agents must provide the following additional information in the incident response plan:

- A plan for how the entity will respond to the activation of the alarm system or information on an intruder in the lab.
- Procedure for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins.

Appendix II. Sample Bomb Threat Checklist

Following is information to be recorded by a bomb threat message recipient during or immediately after the threat is communicated.

- Date/Time
- Time Caller Hung Up
- Phone Number Where Call Was Received

Questions to ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? (Yes, No)
- Why?
- What is your name?
- Where are you?

Record Exact Words of Threat:

_____

_____

Caller's Voice

- ❑ Accent
- ❑ Angry
- ❑ Calm
- ❑ Clearing throat
- ❑ Coughing
- ❑ Cracking voice
- ❑ Crying
- ❑ Deep
- ❑ Deep breathing
- ❑ Disguised
- ❑ Distinct
- ❑ Excited
- ❑ Female
- ❑ Laughter
- ❑ Lisp
- ❑ Loud
- ❑ Male
- ❑ Nasal
- ❑ Normal
- ❑ Ragged
- ❑ Rapid
- ❑ Raspy
- ❑ Slow
- ❑ Slurred
- ❑ Soft
- ❑ Stutter

Background Sounds:

- ❑ Animal Noises
- ❑ House Noises
- ❑ Kitchen Noises
- ❑ Street Noises
- ❑ Booth
- ❑ PA System
- ❑ Conversation
- ❑ Music
- ❑ Motor
- ❑ Clear
- ❑ Static
- ❑ Office machinery
- ❑ Factory machinery
- ❑ Local
- ❑ Long distance

Threat Language:

- ❑ Incoherent Message Read
- ❑ Taped
- ❑ Irrational
- ❑ Profane
- ❑ Well-spoken
- ❑ Machinery
- ❑ Local
- ❑ Long distance

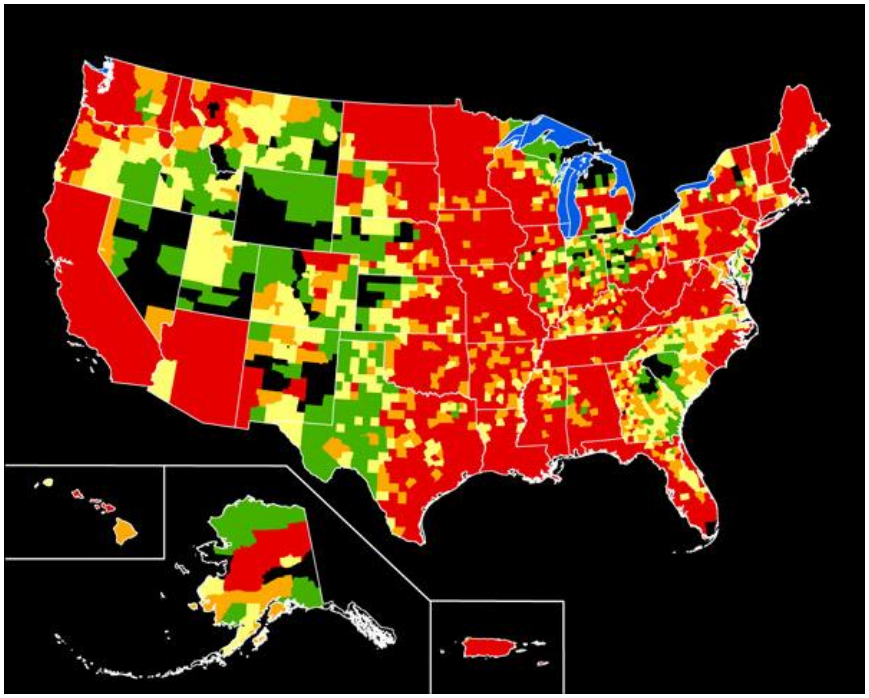
Appendix III. Sample Incident Response Plan Contact Information

Incident Response Plan Contact Information (Section 14)				
Entity Name: **Address:** **City and State:** **SA Registration #:**				
Contact Name	**Work**	**Home**	**Cell**	**Responsibility**
Entity Federal Select Agent Program				
RO				
ARO				
PI #1				
PI #2				
Security				
(Bio)Safety				
CDC				
USDA				
Facility Affiliates				
Owner				
Manager				
Engineer				
Security				
Tenant #1				
Tenant #2				
Facility Support Units				
Electric				
Water				
Gas				
Telephone				
Emergency Response Support				
Police				
Fire				
Rescue				
Medical				
Environmental				
Public Health				

Appendix IV. Evaluating Natural Hazard

Floods

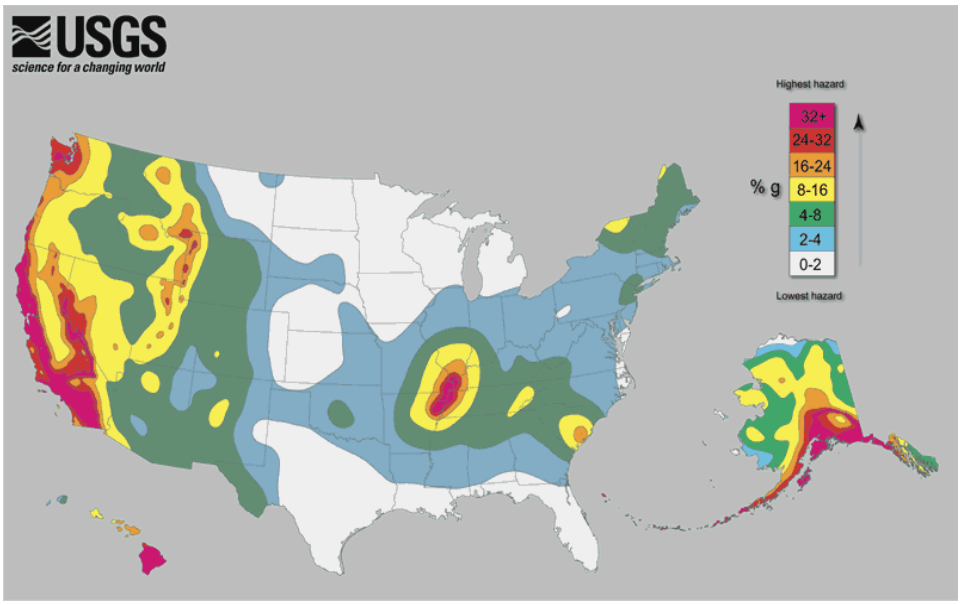
a. Go to the U.S. Geological Survey website (http://www.usgs.gov/) and pull up the most recent map with the Number of Presidential Disaster Declarations for floods.
b. Go to the U.S. Federal Emergency Management website dedicated to floods (http://www.fema.gov/national-flood-insurance-program).
c. The Number of Presidential Disaster Declarations for floods the United States and Puerto Rico shows the areas where a disaster declaration for flooding has occurred in the last 40 years.
d. If your entity is located in a flood plain or in an area where a federal disaster has been declared in the last 50 years make sure you include a section dedicated to floods in your incident response plan.



Presidential disaster declarations related to flooding in the United States, shown by county: Green areas represent one declaration; yellow areas represent two declarations; orange areas represent three declarations; red areas represent four or more declarations between June 1, 1965, and June 1, 2003.

Earthquakes

a. Go to the U.S. Geological Survey website (http://www.usgs.gov/) and pull up the "Seismic Hazard Map of the United States."
b. The map shows relative shaking hazards in the United States and Puerto Rico during a 50-year time period (e.g., the probability of strong shaking increases from very low, to moderate, to high).
c. If your entity is located in a moderate or high area make sure you include an incident response plan for earthquakes.

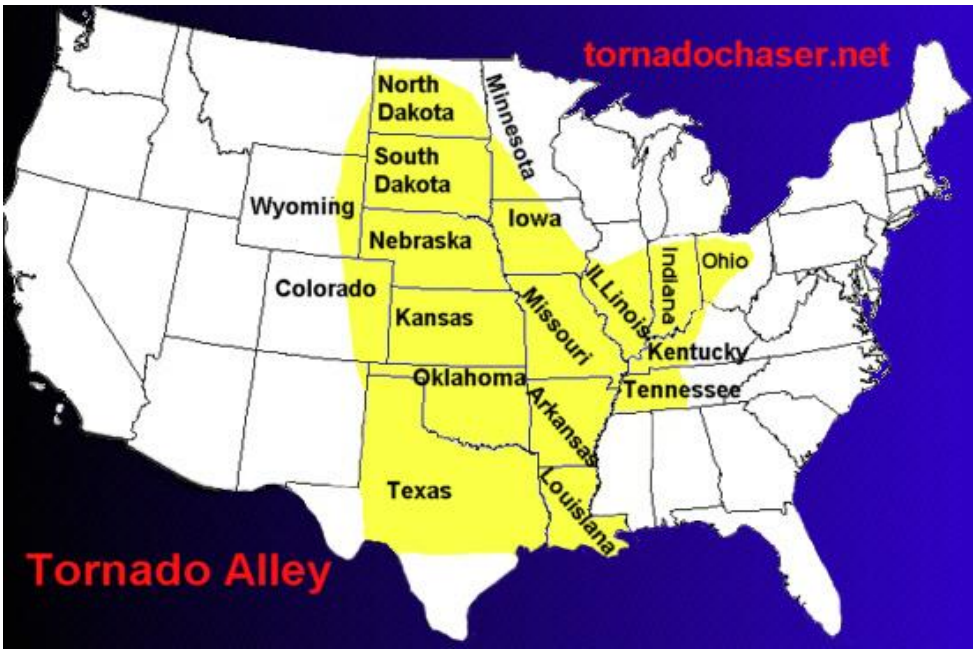


Hurricanes

a. Go to the National Hurricane Center website (http://www.nhc.noaa.gov/) and pull up the 50- year time period map.
b. Click on the "General Climatology" tab on the left side of the home page evaluate the maps, especially the Climatological Areas of Origin and Typical Hurricane Tracks by Month maps.
c. If your entity is located in a moderate or high area make sure you include an incident response plan for hurricanes.
d. You can divide your plan into three parts, 1 for minor and the other for major.
    1) Minor - Minor hurricanes are category 1 and 2. Most buildings built in the coastal area are built to handle a category 2 and below.
    2) Major - Major hurricanes are Category 3 and above. These hurricanes do the most damage.
    3) Other complications - Hurricanes often produce other weather phenomena such as floods and tornadoes. Make sure you account for the expected flooding and hurricanes that accompany hurricanes.

Tornadoes

a. Go to the National Severe Storms Laboratory website (http://www.nssl.noaa.gov/primer/tornado/tor_climatology.html) and pull up Tornado Alley map.
b. The Tornado Alley map displays the areas most susceptible to tornadoes.
c. In addition to the areas highlighted on the Tornado Alley map, all entities within the following states are expected to include tornadoes in their incident management plan: Texas, Oklahoma, Kansas, Nebraska, and Iowa.



Tsunamis

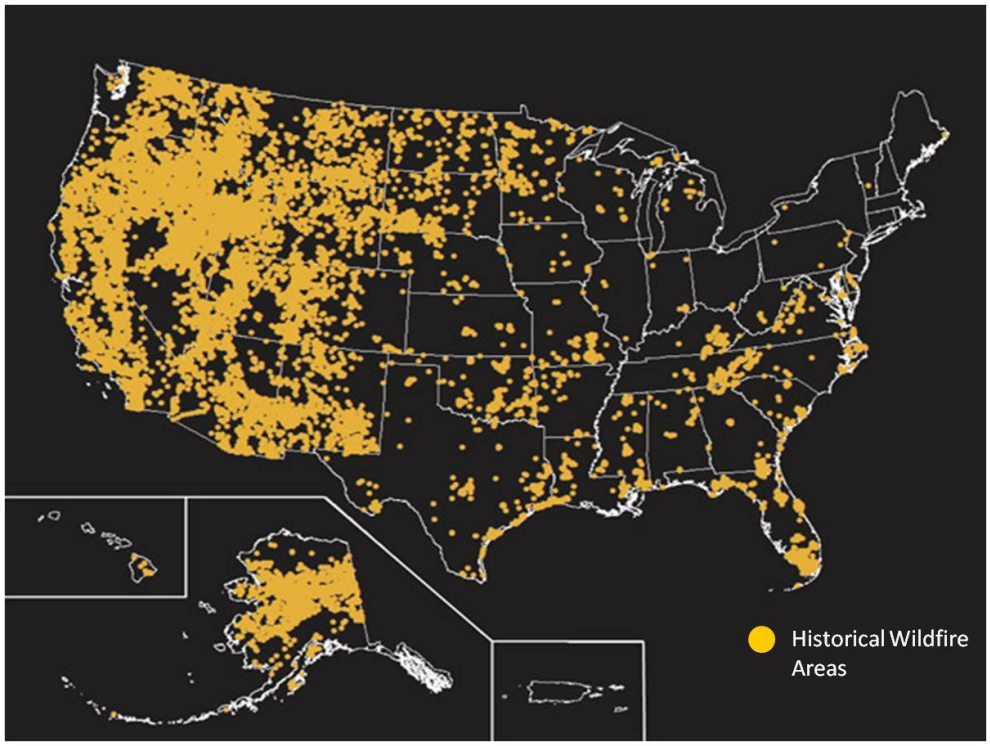
a. Go to the U.S. National Oceanic and Atmospheric Administration website dedicated to tsunamis. (http://www.tsunami.noaa.gov/) and pull up the map that show tsunami events in the US.
b. If your entity is located in a moderate or high area make sure you include an incident response plan for tsunamis.
c. In addition to those entities close enough to be affected by the coast, all entities within 10 miles of the coast should have a tsunami section in their incident response plan.
    1) A tsunami may not affect their entity with water but it could affect traffic into the entity, and personnel who have to go to work.
    2) Evaluate how a tsunami would affect your entity indirectly.

Volcanoes

a. Go to the U.S. Geological Survey website (http://www.usgs.gov/) and pull up a map indicating where the 170 volcanoes are located in the US.
b. If your entity is located within 50 miles of a volcano make sure you include an incident response plan for volcanoes. If you are out of the area of being affected by lava and flying debris you still may be affected by smoke and dark clouds of smut. Make sure your entity is prepared for these possible side effects.

Wildfires

a. Go to the U.S. Geological Survey website (http://www.usgs.gov/) and pull up the latest map which includes wildfires that have affected more than 250 acres.
b. If your entity is located within 15 miles of a volcano make sure you include an incident response plan for volcanoes. If you are out of the area of being affected by direct fire you still may be affected by smoke and dark clouds. Make sure your entity is prepared for these possible side effects.



Low probability/High consequence Events

Entities are encouraged to plan for "low probability/high consequence" events. A low probability/high consequence event is any event which adversely: 1) affects the safety and security of a registered facility; 2) affects human health and safety; and 3) causes environmental degradation. Examples may include high magnitude earthquakes, chemical hazards, radioactive leaks, extreme flooding, or risks an entity is unaware of. An event may lead to a potential failure of key systems such as HVAC, effluent, security or containment systems. Fail-overs may also aggravate the situation (i.e., locks with fail secure may prevent access to the HVAC system). Therefore, entities are encouraged to include procedures in their plan which engages first responders, laboratory staff, the biosafety officer and security personnel in how to respond to these types of events. Having key individuals available and able to talk through the potential impacts will allow better situational awareness. In addition, scenarios in which damage to an entity may have occurred, but the employees are unable to gain access due to evacuations, road blocks, or unsafe conditions should also be considered. First responders may have the ability to assist the entity with access and the safety and security of personnel and assets. If they cannot assist with access, they may assist in assessing the facility for safety or security concerns or completing important tasks such as checking the status of back-up power. The "low probability/high consequence" events portion of the plan should also address the safety of staff during these types of events. In these circumstances, it is critical to know the type of work conducted at the entity during the time of the event. Knowing this will allow the entity to assess the potential for release during and after the event.

Appendix V. Playbook-Scenario Crosswalk for Select Agents and Toxins (compares "Playbook" or SOPs to ensure an entity meets the select agent requirement)

If an entity chooses to adopt a 'playbook' approach (a few SOPs that cover multiple events), it must ensure all select agent requirements are met. This is an example of a simple matrix which correlates the SOPs to the Select Agent requirements to ensure they are met.

For this example, the entity has four SOPs ('plays') which it has mapped back to the select agent requirements.

Incidents Addressed	No notice SOP	Minimal Notice SOP	With Notice SOP	After the Fact SOP	Other
Workplace Violence	X				
Bomb Threats		X			
Suspicious Packages		X			
Natural Disasters					
Earthquake	X				
Hurricane			X		
Flood			X		
Tornado		X			
Severe Weather (Winds/Storm)		X			
Severe Storm (Ice, Snow)			X		
Fire		X			
Gas Leak		X			
Explosion	X				
Information Systems Breach					X
Power Outage	X				
Security Breaches/ Suspicious Activity				X	
Inventory Discrepancies				X	
Theft, Loss, Release					X
Directed Evacuation		X	X		

Appendix VI. Scenario-Plan Crosswalk (compares multiple organizational plans ensure an entity meets the select agent requirement)

If the entity consolidates existing plans into an incident response SOP, it must also be mapped back to the select agent requirements. This matrix assists in the mapping.

	Does the incident response plan cover:	SOP Number/Name	Date Modified	Remarks
Workplace Violence	Yes/No			
Bomb Threats	Yes/No			
Suspicious Packages	Yes/No			
Natural Disasters	Yes/No			
Fire	Yes/No			
Gas Leak	Yes/No			
Explosion	Yes/No			
Information Systems Breach	Yes/No			
Power Outage	Yes/No			
Security Breaches/ Suspicious Activity	Yes/No			
Inventory Discrepancies	Yes/No			
Theft, Loss, Release	Yes/No			
Annual Training	Yes/No			

Appendix VII. Natural Disaster External Coordination Chart

Event & Source	Source	Severity	Externalities	Incident Plan	Post Response
Tropical Weather	**State EOC*, www.noaa.gov and local media**	Tropical Storm	Floods, Tornadoes, power outage		
	State EOC*, www.noaa.gov and local media	Hurricane Category 1 & 2	Storm Surge, Floods, Tornadoes, power outage		
	State EOC*, www.noaa.gov and local media	Hurricane Category 3 & 4	Storm Surge, Floods, Tornadoes		
Earthquake	**State EOC*, www.usgs.gov, local and national media**	5.0 – 6.4	Power Outage, Infrastructure Damage; Gas Leaks		
	State EOC*, www.usgs.gov, local and national media	6.5 or greater	Power Outage, Infrastructure Damage; Gas Leaks		
Tornado	**State EOC*, local and national media**	Any tornado	Power Outage; Infrastructure Damage		
Flood	**State EOC*, local and national media**	Any flood near and entity	Power Outage, Infrastructure Damage		
Volcano Eruption	**State EOC*, local and national media**	Any eruption near an entity	Too much dust in HEPA Filters; Fire		
Wildfire	**State EOC*, local and national media**	Any wildfire near an entity	Too much smoke in HEPA Filters		

- * - State Emergency Operation Centers (EOCs)- will likely have information on predicted paths, expected damages, evacuation routes, damage to infrastructure, federal and state declaration

Appendix VIII. Incident Response Plan Validation

Does the Plan(s) Contain:

	Yes	No
(1) The name and contact information (e.g., home and work) for the individual or entity (e.g., responsible official, alternate responsible official(s), biosafety officer, etc.), (2) The name and contact information for the building owner and/or manager, where applicable, (3) The name and contact information for tenant offices, where applicable, (4) The name and contact information for the physical security official for the building, where applicable, (5) Personnel roles and lines of authority and communication, (6) Planning and coordination with local emergency responders, (7) Procedures to be followed by employees performing rescue or medical duties, (8) Emergency medical treatment and first aid, (9) A list of personal protective and emergency equipment, and their locations, (10) Site security and control, (11) Procedures for emergency evacuation, including type of evacuation, exit route assignments, safe distances, and places of refuge, and (12) Decontamination procedures.		

Does the Plan(s) Cover:

	Yes	No
(1) Theft, loss, or release of a select agent or toxin (2) Inventory discrepancies (3) Security breaches (including information systems) — (1) Entities with Tier 1 Agents must cover FBI notification process for reporting of thefts or Suspicious Activity that may be criminal in nature. (4) Severe weather and other natural disasters (5) Workplace violence (6) Bomb threats (7) Suspicious packages (8) Emergencies such as fire, gas leak, explosion, power outage		